Abridged Translation of Cited Reference

Reference 3:

Publication No.: JP-A-2002-526822 (WO0019299)
Date of Publication: August 20, 2002
Application No.: 572741/'00
Date of Application: September 25, 1998
Convention Priority: None
Applicant: HUGHES ELECTRONICS CORP (US)
Inventors: CASSAGNOL ROBERT D, et al.
Title of the Invention: AN APPARATUS FOR PROVIDING A SECURE PROCESSING ENVIRONMENT

[0032]:

A device 10 comprises a processor 16 (refer to Fig.2) to control an operation of the device 10. One function of the processor 16 is to operate no less than two security sell. A first security sell is called as a kernel mode sell, and it is desirable that the security sells are operating during sensitive confidential information is accessed, processed, and enabled on an internal bus of the device 10. A second security sell is called as a user mode sell, and the user mode sell is operated when an access to the sensitive data is not allowed. When the kernel mode is enabled, the processor 16 is not limited regarding an access to hardware or software in the device 10. Thereby, it is prevented that an external pin of the device 10 discovers sensitive information which shows at least one of the operation executed by the device 10 or the information processed by the device 10. When the user mode is executed, the processor 16 is added a limitation of an enhanced level to an operation in the device 10, while the limitation is not added to an operation which is visible externally. However, it is desirable that an execution limitation of hardware is maintained in both security sell.

[0064]:

The device 10 uses at least two security sell, i.e. a kernel mode sell and an user mode sell. The processor 16 operates a non-confidential software in the user mode, and operates a confidential software in the kernel mode. The two security cell is sufficient for many applications. However, it is desirable that a multiple task among many secret tasks is available. It is also desirable that a protection between no less that two cells which execute software simultaneously (for example, access systems having different conditions from different bender), and desirable to prevent that all systems are damaged by one cell which is processed by compromise.